SQUIRE PATTON BOGGS

Facial Recognition in the Spotlight Again

What the Privacy Commissioner's Investigation Into Kmart Has Taught Us

Australia – September 2025

The privacy commissioner has determined that Kmart's use of facial recognition technology (FRT) to prevent returns fraud is in breach of Australian privacy law.

Consumer group CHOICE raised concerns about Bunnings, Kmart and the Good Guys' use of FRT back in 2022, which prompted the privacy commissioner to launch her own investigation into the retailers' practices. This latest determination builds on the privacy commissioner's earlier findings against Bunnings' use of FRT in October 2024.

As Commissioner Kind noted in her accompanying blog post, these determinations are not intended to ban the use of FRT altogether. Instead, they provide new guidance on how the *Privacy Act 1988* (Cth) (Privacy Act) applies to the deployment of FRT in retail environments. We review the commissioner's decision to help contextualise what it may mean for Australian businesses and the future use of emerging technologies.

Background

Between 22 June 2020 and 22 December 2021, Kmart rolled out FRT across 28 of its national stores as part of prevention measures to combat in-store refund fraud.

How Did Kmart's FRT System Work?

The system combined Kmart's CCTV cameras with third-party software, capturing five to six images of each individual as they entered the store or approached the returns counter. Those images were compared against a database of "persons of interest", which included individuals identified at that store, as well as customers from other locations whom Kmart believed might engage in refund fraud across stores.

If the system suggested a match, staff were notified and could use this information to help detect return fraud. Images that did not match a person of interest were not accessible to Kmart staff and were deleted after a period of time (the exact period was redacted in the decision). Kmart also told the commissioner that, to the best of its knowledge, no child's data was ever included in the database.

In this scenario, using facial information captured through CCTV to identify persons of interest – or, in the case of nonmatches, exclude persons who were not of interest – meant that those images were classified as sensitive information under the Privacy Act. "Sensitive information" is defined to include biometric information that is used to identify an individual, as distinct from other individuals (even without details such as their name).

What do privacy laws say about FRT?

Well, nothing explicitly. As stated in the commissioner's blog post, "the Privacy Act is technology-neutral." Put simply, the law does not single out or regulate specific technologies like facial recognition, AI or CCTV.

Instead, the act sets out principles-based rules (the Australian Privacy Principles, or APPs) that apply regardless of what technology or mechanism is used. So, whether an organisation collects personal information using paper forms, a database, CCTV or FRT, the same obligations apply. Among these:

- Sensitive information can only be collected with consent (APP 3), unless an exemption applies.
- Individuals must be notified about the collection of personal information and its purpose (APP 5).
- Use and disclosure is usually limited to the purpose for which the information was collected, unless an exemption applies (APP 6).

The Investigation

Kmart's Argument for FRT

Recognising that it had not obtained individuals' consent to the collection of their biometric information, Kmart argued it could rely on the "permitted general situation" (PGS) exemption in Section 16A of the Privacy Act, which allows sensitive information to be collected without consent where any one of a set of limited circumstances apply. We discuss the relevant PGS below.

Kmart maintained that FRT allowed staff to assess whether an individual was a person of interest and, after also determining if any "suspicious circumstances" existed, whether to process the return.

The Commissioner's Determination

Kmart sought to rely on the second PGS listed in Section 16A. To successfully do so, Kmart needed to establish that:

(a) It has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in.

(b) It reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.

Against the first consideration, the commissioner accepted that refund fraud constituted unlawful activity and that Kmart had reasonable grounds to suspect it was happening in its stores.

However, the commissioner determined that Kmart did not satisfy condition (b) of the exception.

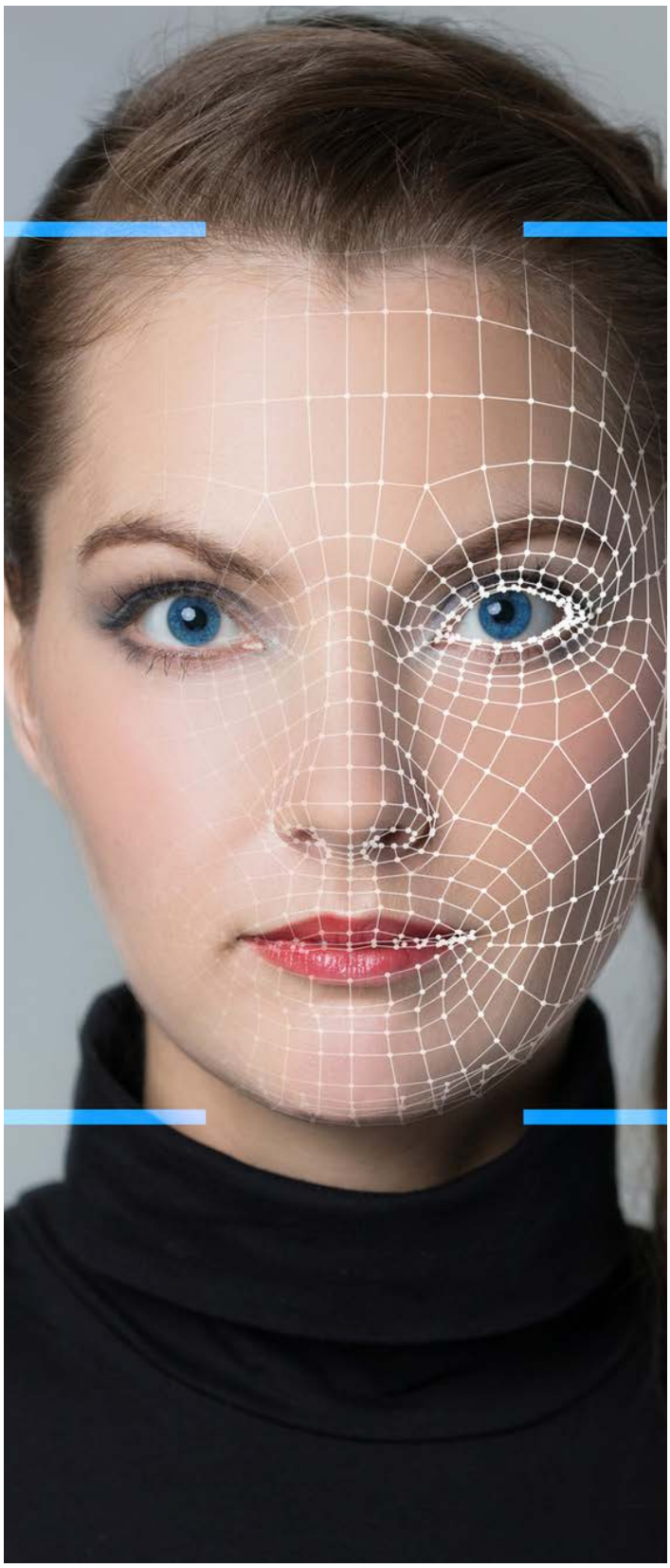
Appropriate Action

While not critical to the decision, the privacy commissioner expressed doubt as to whether Kmart's use of the FRT system to identify persons of interest constitutes "appropriate action" in relation to combatting return fraud. While output from the system gave staff the confidence and ability to refuse refund requests and also reduced the likelihood of those customers behaving in a threatening manner when approached, these ultimately were only benefits and conveniences. FRT did not enable staff to detect return fraud, but it provided a matching system which made it easier for them to ascertain whether fraud was likely to have taken place. This was the appropriate action taken by Kmart in relation to unlawful activity.

Necessary and Proportionate

The commissioner accepted that Kmart management did subjectively believe that FRT was necessary to take appropriate action in relation to retail fraud. However, the commissioner stressed that the test is not only about genuine belief, but also about whether there are reasonable grounds, based on objective facts, to show the collection was necessary. The commissioner found that, in this use case, FRT was helpful and convenient, but it was not the only or the best way to investigate or address refund fraud. Other less privacy-intrusive – but still "practical and effective" – measures existed, such as additional staff oversight, changes to the location of return counters, RFID tags or a stricter refund policy. In addition, while much of the relevant evidence was redacted from the decision, the commissioner found that there were "significant practical limitations" to FRT in detecting every kind of return fraud and that even in the subset of cases where it was effective, there was an "element of uncertainty" in its findings.

As in her *Bunnings* determination, the commissioner concluded that Kmart's collection of biometric data from every individual entering the store (as well as the subset of those individuals who also approached the returns counter) was disproportionate, in light of the harm against which Kmart was trying to protect and the other methods available to it.



Takeaways

Regulatory priorities are shifting, and organisations should expect continued scrutiny of biometric deployments against privacy laws. The Office of the Australian Information Commissioner (OAIC) has listed rights-preservation in new and emerging technologies as one of its four regulatory action priorities for 2025-26, explicitly citing FRT and biometric scanning as relevant technologies.

For businesses exploring FRT, there are ample takeaways from the recent *Kmart* ruling. Perhaps the most significant are:

1. Pilots are not immune from scrutiny.

Kmart's FRT was deployed as a pilot. The commissioner acknowledged that Kmart can still hold a "reasonable belief" that FRT is necessary without "qualitative proof", but made clear that trial status does not excuse noncompliance with the Privacy Act. By contrast, New Zealand's recent Biometric Processing Privacy Code expressly allows organisations to defer compliance with the requirement that biometric processing is "necessary" for a specific purpose while they are conducting a trial of the technology.

Note – Unlike Australia, New Zealand's privacy framework does not require consent to the processing of sensitive information or apply the same restrictive exemptions to obtaining consent.

2. Necessity remains the threshold test.

The commissioner accepted that refund fraud was unlawful but found that FRT was not necessary to address it. Convenience and efficiency – though buzzwords for the adoption of technology in workplaces – do not sufficiently meet the necessity threshold. Less intrusive alternatives that are still "practical" and "effective" should be assessed before FRT is deployed.

3. Document, document, document!

While it may not necessarily have changed her decision, the commissioner specifically noted that there was no evidence of "project planning documents or a privacy impact assessment having been conducted prior to the implementation of the FRT pilot program" to establish both that FRT was necessary, and the basis on which other available options were shown to be impractical or ineffective.

4. Privacy law and advancements in tech can co-exist…

From a technology perspective, retailers may feel disincentivised from trialling emerging tools like FRT. Yet Commissioner Kind has been clear that she is not seeking to ban innovation outright. As the commissioner noted, her office has so far only examined two retail deployments. Other uses are already underway in Australia, including at airports and in gaming environments where FRT is sometimes mandated by law to support gambling self-exclusion schemes. The message is that innovation is possible, but only where necessity, proportionality and transparency can be demonstrated from the outset.

5. …but certain retail use cases are under siege.

In her accompanying blog post, the commissioner states that "in the absence of parliamentary authorisation to specifically authorise the use of FRT without consent," she must bring to bear the considerations that she has set out in her *Bunnings* and *Kmart* decisions to the use of these emerging technologies.

At least to us, this seems an acknowledgment that for certain retail use cases, the deployment of FRT will be difficult to justify. This has been backed up by other statements made by the commissioner, where she has indicated that FRT may be acceptable in a retail scenario where users are better able to consent to its use. For example, the size and nature of luxury goods stores may mean that staff are better able to obtain consent from visitors to the use of FRT.

Even so, we think there is a large space of potential permitted scenarios that sit between airport use (at one end) and the *Kmart*/*Bunnings* decisions (at the other). We look forward to working with our clients to help advise on these.

Authors

Tanvi Mehta Krensel
Partner, Sydney
T +61 2 8248 7810
E tanvi.mehtakrensel@squirepb.com

Eman Mourad
Paralegal, Sydney
T +61 2 8248 7831
E eman.mourad@squirepb.com